



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
Washington, D.C. 20231
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/127,767	07/31/1998	SARVAR PATEL	2925-0161P	1713

30594 7590 05/22/2002

HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 8910
RESTON, VA 20195

EXAMINER

CALLAHAN, PAUL E

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 05/22/2002

12

Please find below and/or attached an Office communication concerning this application or proceeding.



UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

RECEIVED

MAY 21 2002

Group 2100

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Paper No. 12

Application Number: 09/127,767

Filing Date: February 23, 2000

Appellant(s): Sarvar Patel

John A. Castellano

Registration No. 35,094

For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed March 7, 2002.

(1) *Real Party in Interest*

A statement identifying the real party in interest is contained in the brief.

(2) *Related Appeals and Interferences*

A statement identifying the related appeals and interferences which will directly affect or be directly affected by or have a bearing on the decision in the pending appeal is contained in the brief.

(3) *Status of Claims*

The statement of the status of the claims contained in the brief is correct.

(4) *Status of Amendments After Final*

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) *Summary of Invention*

The summary of invention contained in the brief is correct.

(6) *Issues*

The appellant's statement of the issues in the brief is correct.

(7) *Grouping of Claims*

Appellant's brief includes a statement that claims group 1: 12, 14, 15, 18-20; group 2: 13, 16; group 3: 17; group 4: 21, 22; group 5: 1-3, 5, 6, 11, group 6: 4, 9; group 7: 7, 8; group 8: 10 do not stand or fall together and provides reasons as set forth in 37 CFR 1.192(c)(7) and (c)(8).

Art Unit: 2132

(8) *Claims Appealed*

The copy of the appealed claims contained in the Appendix to the brief is correct.

(9) *Prior Art of Record*

The following is a listing of the prior art of record relied upon in the rejection of claims under appeal.

“Handbook of Applied Cryptography,” Alfred Menezes, Paul van Oorschot, Scott Vastone, CRC Press Inc. 1997. pp. 397-404

(10) *Grounds of Rejection*

The following ground(s) of rejection are applicable to the appealed claims:

Claims 1-22 rejected under 35 U.S.C. 103(a) as being obvious over “Handbook of Applied Cryptography,” Menezes, Oorschot, and Vanstone, CRC Press 1997, pp. 397-404.. This rejection is set forth in prior Office Action, Paper No. 6.

(11) *Response to Argument*

Appellant's brief includes a statement that the claims in groups 1-8 do not stand or fall together and provides reasons as set forth in 37 CFR 1.192(c)(7) and (c)(8).

Group 1: Claims 12, 14, 15, and 18-20.

The Applicant argues that the Examiner failed to provide the requisite showing of a teaching or motivation for the proposed modification of incorporating the sequence number (counter value) taught by Menezes on page 397 Sec. 10.3.1 and 10.9, and page 399 sec. 10.12(ii) Sequence Numbers, into the SKID3 algorithm taught on page 402 sec. 10.17(ii) Challenge-Response based on (keyed) One-Way Functions. The Applicant asserts that “...the Examiner has failed to point out the specific portion of Menezes et al. Which would teach or motivate one to replace random numbers with sequence numbers (i.e count values) in the

Art Unit: 2132

SKID3 authentication algorithm.” The Examiner respectfully counters that the motivation to combine the teachings of a sequence number into the SKID3 algorithm is found in page 397 sec. 10.9 of the Menezes reference where the author states “It typically serves to prevent undetectable replay attacks in challenge-response mechanisms. This was specifically cited on paragraph 6 of the previous Office Action in this case, paper no. 6. In addition to this, the Examiner’s rejection of the claims includes a discussion of the motivation to combine on page 7 and page 8 of the Office Action where the Examiner states: “...one of ordinary skill in the art would have known replay attacks were used to subvert challenge-response authentication protocols, and therefore would have been familiar with choosing one of the three above options.” The Examiner respectfully disputes the Applicant’s contention that these are merely conclusionary statements.

The Applicant argues that the proposed modification to Menezes et al. Fails to anticipate the instant invention because the use of a sequence number as disclosed by Menezes in a mutual authentication algorithm such as SKID3 would fail to anticipate the outputting of a first challenge. The Applicant further asserts on page 16 of the Brief that Menezes only teaches the use of a SKID3 algorithm to perform one-pass authentication in which only one message is sent between the parties during authentication because the verifying party does not send a first challenge to the party being authenticated. Applicant states that this algorithm is found on page 401 of the Menezes reference. The Applicant is referring to a single-pass algorithm on page 401 of the Menezes reference that was not relied upon in the rejection of the claims.

The algorithm which was cited and relied upon in the rejections was the SKID3 algorithm found on page 402 of the Menezes reference under section 10.17(ii) Challenge-Response based on (keyed) One-Way Functions. This is cited explicitly on page 7 of the previous Office Action in this case. This is a three-pass SKID3 algorithm which does utilize a first and a second challenge r_A and r_B which are taught as a random

Art Unit: 2132

number and a counter value respectively as discussed infra. The Applicant later refers on page 16 of the Brief to the SKID3 algorithm found on page 402 of the Menezes reference as the one cited by the Examiner in the rejection of the claims.

The Applicant asserts that the amount of overhead required by the use of sequence numbers is such that "...it allows a verifying party to match the sequence number it expects to receive from a party requesting authentication with that which it actually receives. Since Menezes teaches that each party knows which sequence number will be used for verification, the verifying party does not issue the sequence number as a challenge to the other party. The Examiner respectfully counters that this mechanism is not taught by Menezes and that the SKID3 algorithm found on page 402 does indeed send a challenge that is a sequence number as per the discussion on 398 and 399 especially in section 10.12(ii) Sequence Numbers.

The Applicants assertion that the SKID3 algorithm taught by Menezes reference would have to omit the rA challenge value found on page 402 if it were a sequence number is not supported by the actual teachings of the Menezes reference. The challenge value rA is taught by Menezes as interchangeably a random value and a challenge number as discussed supra. Menezes does not teach that the values rA and rB must be exclusively random values or sequence numbers exclusively.

Group II: Claims 13 and 16.

The Applicant argues that the SKID3 algorithm as taught by Menezes on page 402 fails to anticipate the Applicant's claims 13 and 16 because both of the claims require that a second key be established based upon the first and second challenges. In response, the Examiner respectfully counters that the SKID3 algorithm on page 402 of Menezes calculates, as a final step, a new value based upon the first and second challenges: $hK(rB, rA, A)$. It is very common in the art of cryptographic authentication for this type of value

Art Unit: 2132

to be used as a cryptographic key. For example, reference is made on page 499 to a well known Authenticated Key Exchange Protocol 2 (AKEP2) where a keyed hash function $h'K'$ of the same type as hK in the SKID3 protocol is taught as being further used as an encryption key. Additional examples of the use of a keyed hash function $h'K'$ as an encryption key are referenced in the "Notes and Further References" section at the end of the chapter from the Menezes reference that was used to teach the SKID3 protocol, specifically on page 535, sec. 12.3, 1st paragraph. Therefore under a reasonably broad interpretation, the Applicant's claim language would be rendered obvious by this final value calculated in the SKID3 algorithm of Menezes. The Applicant asserts that Menezes does not establish a second key as required by claims 13 and 16 however the calculated value $hK(rB, rA, A)$ is a second key value different from the first key K and does render obvious the Applicant's claim language.

Group III: Claim 17

The Applicant presents essentially the same argument in traverse of the rejection of claim 17 as was offered to traverse that of claims 13 and 16. The Applicant asserts that a second key is not established by the Menezes SKID3 protocol. The Examiner respectfully counters that such is taught by the calculated value $hK(rB, rA, A)$. It is common in the art of cryptographic authentication for this type of value to serve as an encryption key.

Group IV: Claims 21 and 22

The Applicant's arguments in traverse of the rejections of claims 21 and 22 is persuasive and therefore the rejections of these claims is overcome.

Art Unit: 2132

Group V: Claims 1-3, 5, 6, and 11

The Applicant argues that claim 1 may be distinguished from the teachings of the Menezes reference because there is no teaching or suggestion to increment the sequence number or count value of Menezes in response to the first challenge. The Examiner respectfully counters that the sequence number taught by Menezes on page 397 sec. 10.3.1 are specifically taught as non repeating or time varying. Additionally on page 399 sec. 10.12(ii) "Sequence Numbers" they sequence numbers are taught as being used only once and are then incremented: "The simplest policy is that a sequence number starts at zero, is incremented sequentially, and each successive message has a number one greater than the previous one received." Therefore upon receipt of the first challenge in the SKID3 protocol taught on page 402 of Menezes, the sequence number must be changed after it's use so that it will be used only once as taught by Menezes on page 399 sec. 10.12(ii).

Group VI: Claims 4 and 9

The Applicant refers to the Argument presented in traverse of the rejections of claims 13 and 16 and traverses the rejections of claims 4 and 9 on the same grounds. The Examiner counters with the arguments presented Supra in the discussion of claims 13 and 16.

Group VII: Claims 7 and 8

The Applicant presents the same arguments in traverse of the rejections of claims 7 and 8 as were presented for claims 21 and 22. The argument is persuasive for claims 7 and 8 as well and the rejections of the claims is overcome.

Art Unit: 2132

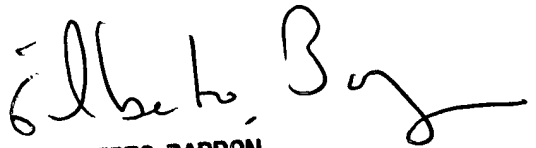
Group VIII: Claim 10

The Applicant refers to the argument presented in traverse of the rejection of claim 17 in traverse of the rejection of claim 10. The Examiner refers to the counter argument presented supra in the discussion of claim 17 in response.

Appeals Conference Held 5/17/02

Conferees:

Gilberto Barron, SPE Art Unit 2132: Cryptography


GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Thomas Peeso, Primary Examiner, Art Unit 2132

Paul Callahan, Examiner, Art Unit 2132

Paul Callahan